FOLEY LARDNER
ATTORNEYS AT LAW

IDENTITY THEFT

By: Andrew Serwin

Identity Theft

by: Andrew Serwin

Preventing identity theft has been one of the primary goals of the Federal Trade Commission, the federal agency charged with consumer protection. While the FTC has taken action to protect consumers' private information, there is no generally applicable national standard for data protection. Instead, the federal approach has been to pass laws that protect specific types of private information, such as medical or financial information.

Citing a 108 percent increase in identity theft crimes, the California Legislature rejected this approach by enacting a law that became effective July 1. Civil Code Section 1798.82 will have a major impact on California companies and may ultimately become the de facto national standard. Moreover, many non-California companies will be forced to comply with Section 1798.82 because it codifies new requirements regarding data security that apply to any person or business that "conducts business" in California, whether headquartered in California or not.

Disclosure by Data Owners

Section 1798.82 mandates two different disclosures if a breach of data security occurs. The first, and most burdensome, is applicable if a person or business: (i) conducts business in California; (ii) owns or licenses unencrypted computer data; and (iii) the computer data contains "personal information" regarding a resident of California. Personal information is defined by the statute as either an individual's first name or middle initial combined with a last name, and: (a) a social security number; (b) a California Driver's License number or Identification Card number; or (c) an account number or credit or debit card number and the Personal Identification Number (PIN), security code or password that would permit access to the account.

If there is a security breach of a system that contains "personal information," and it is known or reasonably believed that personal information has been acquired by an unauthorized individual, then the data owner must make a disclosure of the security breach to the affected California residents. While certain terms are defined by the statute, "acquisition" of information is not. This creates a compliance standard that data owners must face with little guidance. Does acquisition mean that the electronically stored information was downloaded? Or does it mean that the information was merely viewed? Data owners are faced with this disclosure dilemma because acquisition can occur in a manner that doesn't create a separate and definitive record of acquisition. For example, there would be no electronic record of acquisition if someone viewed the information and manually inputted it into their computer, or even simply wrote it down. This would clearly be an acquisition, but it would be impossible to determine electronically that anything more than access had occurred. The answer to this question is all the more ambiguous given the somewhat amorphous "reasonable belief" standard in the statute.

Disclosure to the affected individuals must be made as expediently as possible, and without unreasonable delay, unless there is a concern that disclosure will impede a criminal investigation. This requirement raises another potential issue, which is whether the statute creates an implicit duty to involve law enforcement in order to determine whether disclosure will affect an investigation. While there is no explicit requirement, there may be certain situations that would require disclosure to law enforcement in order to obtain clearance for disclosure. Disclosure must be made in one of three statutorily mandated methods. The first option is written notice to the affected individual. The second option is electronic notice, but only if the notice complies with certain federal statutes regarding electronic signatures, Title 15 U.S.C. ß 7001. A third alternative is applicable if it is shown that: (i) the cost of providing notice would exceed $250,000; (ii) the class of affected persons exceeds 500,000 people, or (iii) the person or business does not have sufficient contact information to provide notice.

If one of these three factors exists, then substitute notice can be given via three new and different options. The first is notice via e-mail. The second alternative is "conspicuous" posting on a Web site. The third alternative is notification to major statewide media.

Disclosure by Entities that Maintain Data

While the majority of the statute addresses disclosures required by the data owner, the second disclosure requirement applies to individuals or companies that merely maintain a data owner's computerized data. Persons or companies that maintain others' data are also required to disclose a breach of their security that results in the unauthorized acquisition of personal information. However, the person or entity that maintains the data is not required to make a disclosure to California residents, but rather to the data owner.

Existing Security Policies

While Section 1798.82 offers little discretion regarding these disclosures, one portion of the statute may offer some relief from strict compliance with these requirements. Section 1798.82 does permit data owners to continue using their own disclosure regimes if they are part of a broader information security policy, but only if the policy is consistent with the timing requirements of the statute.

Compliance Concerns

There are a number of potential problems faced by those that must comply with Section 1798.82, as well as the courts that must enforce it.

The first hurdle is that Section 1798.82's protections cannot be waived. In many situations, consumers are afforded the option of waiving certain statutorily mandated protections when they enter commercial transactions. This is permitted because in most circumstances it is recognized that the parties to an agreement should have the autonomy to self-regulate the terms of their contractual relationship. However, the California Legislature has eliminated consumers' ability to make this choice because Section 1798.83 renders any waiver of the Section 1798.82 protections unenforceable.

Another difficulty facing data owners is that the law can be violated unknowingly. This situation will likely arise because while a company may know that there was compromise of a database, a company will not know in all situations that a California resident's information was acquired. The definition of personal information in the statute includes information that does not necessarily reveal a person's state of residence, particularly if the only address possessed by the data owner is an e-mail address. The statute does not require the data owner know a California resident's data was acquired, but only that there was an acquisition of data. As such, the data owner is in the difficult position of either violating the law, or disclosing unauthorized acquisition to individuals who are not known to be California residents.

Methods of Enforcement

Consumers are permitted to bring actions for injunctive relief against businesses that either violate the law, or propose to violate the law. In other words, even if a business has not yet violated the law it can be subject to an enforcement action if it appears to a California consumer that the business might, at some future date, violate the law.

Another California statute, Business and Professions Code Section 17200 et. seq. (the UCL), may be the main vehicle for litigation arising from violations of Section 1798.82. The UCL permits an individual to sue on behalf of him or herself, as well as all other affected individuals in what is, in essence, an uncertified class action. This is true even where the named plaintiff was not in any way affected by the alleged conduct. Moreover, unlike other comparable doctrines, the UCL does not require a finding of intent. Instead, there is strict liability for a violation of the UCL. The UCL is also of concern to out-of-state and foreign companies because a claim under the UCL can be stated even if the alleged conduct occurs out-of-state so long as it affects California residents.

The UCL prohibits any unlawful, unfair or fraudulent business act or practice, or unfair, deceptive, untrue or misleading advertising. An unlawful act includes anything that properly can be called a business practice or act and is also "forbidden by law." An act is unlawful as defined by the UCL if it is prohibited by any law whether the law is "civil or criminal, federal, state, or municipal, statutory, regulatory, or court made."

Given the requirements of Section 1798.82 and broad nature of the UCL, a California resident could bring an uncertified class action on behalf of the general public alleging an unlawful business practice based upon the violation, or proposed violation, of Section 1798.82. In addition to obtaining monetary and injunctive relief under the UCL, the person bringing the lawsuit on behalf of the general public is statutorily entitled to recover attorneys' fees in certain cases.

Potential Solutions

Any data owner that does business in California must implement procedures to comply with this law. The first option available to data owners is to encrypt personal data. If the personal information is encrypted then the notice requirements of Section 1789.82 are inapplicable. Moreover, data owners should consider eliminating the unnecessary storage of personal information in order to decrease the risk of unauthorized acquisition. Security of networks should also be increased to reduce the possibility of a security breach. Also, companies should consider establishing policies and procedures for security incidents that include a predetermined list of company contacts who are given immediate notice of any security incident.

One thing is clear – given the potential financial incentives of litigation, California courts will be forced to address these issues in the very near future.